

Blue Team Tools: Defense against Adversary Activity Using MITRE Techniques



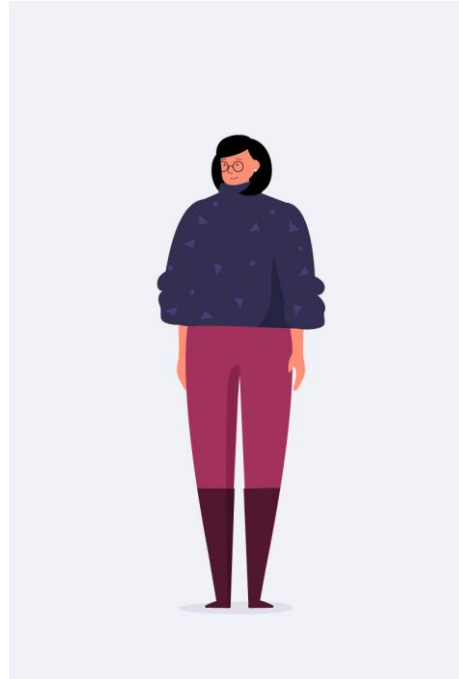
Aaron Rosenmund

AUTHOR EVANGELIST - INCIDENT RESPONSE

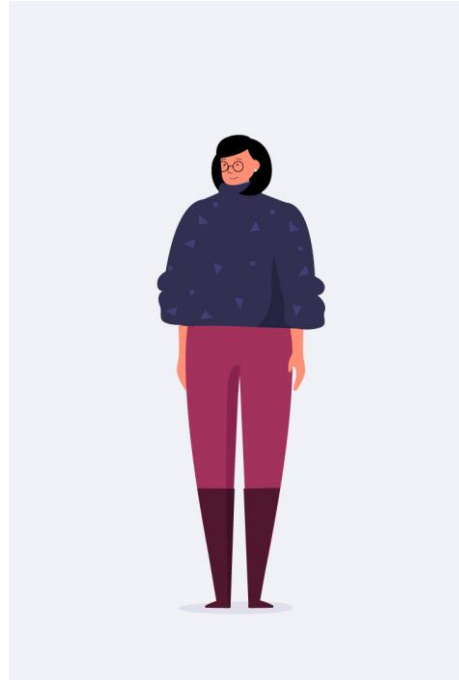
@arosenmund www.aaronrosenmund.com



The Story Starts and Ends with You



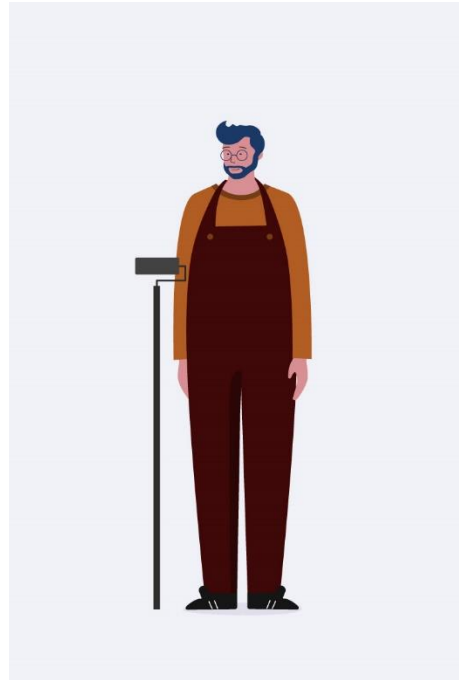
The Story Starts and Ends with You



**Blue Team
Operator**



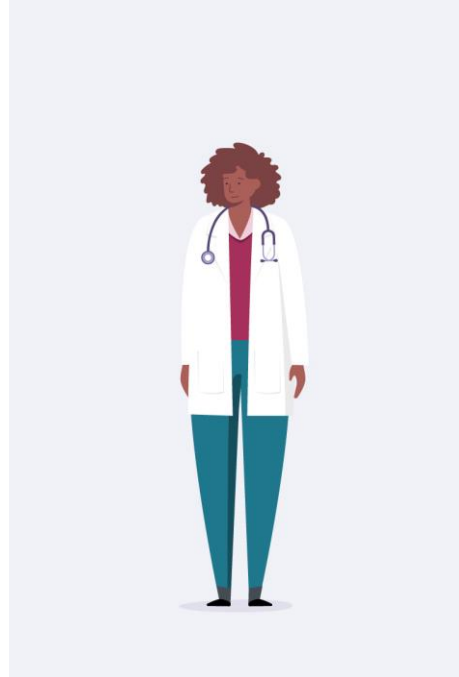
The Story Starts and Ends with You



Security
Engineer



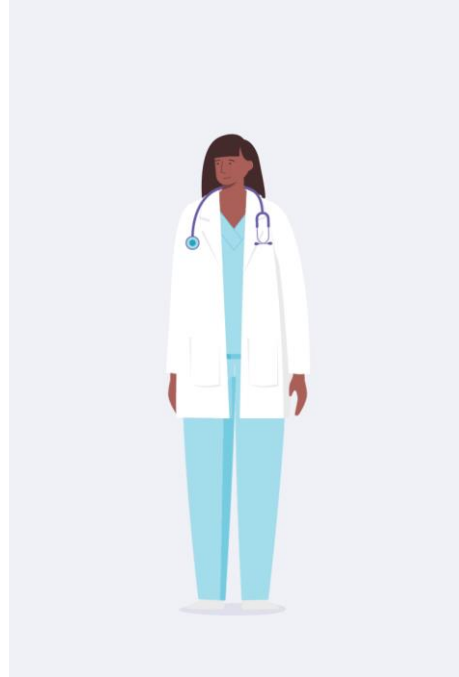
The Story Starts and Ends with You



Security Analyst



The Story Starts and Ends with You



**Incident
Responder**



The Story Starts and Ends with You



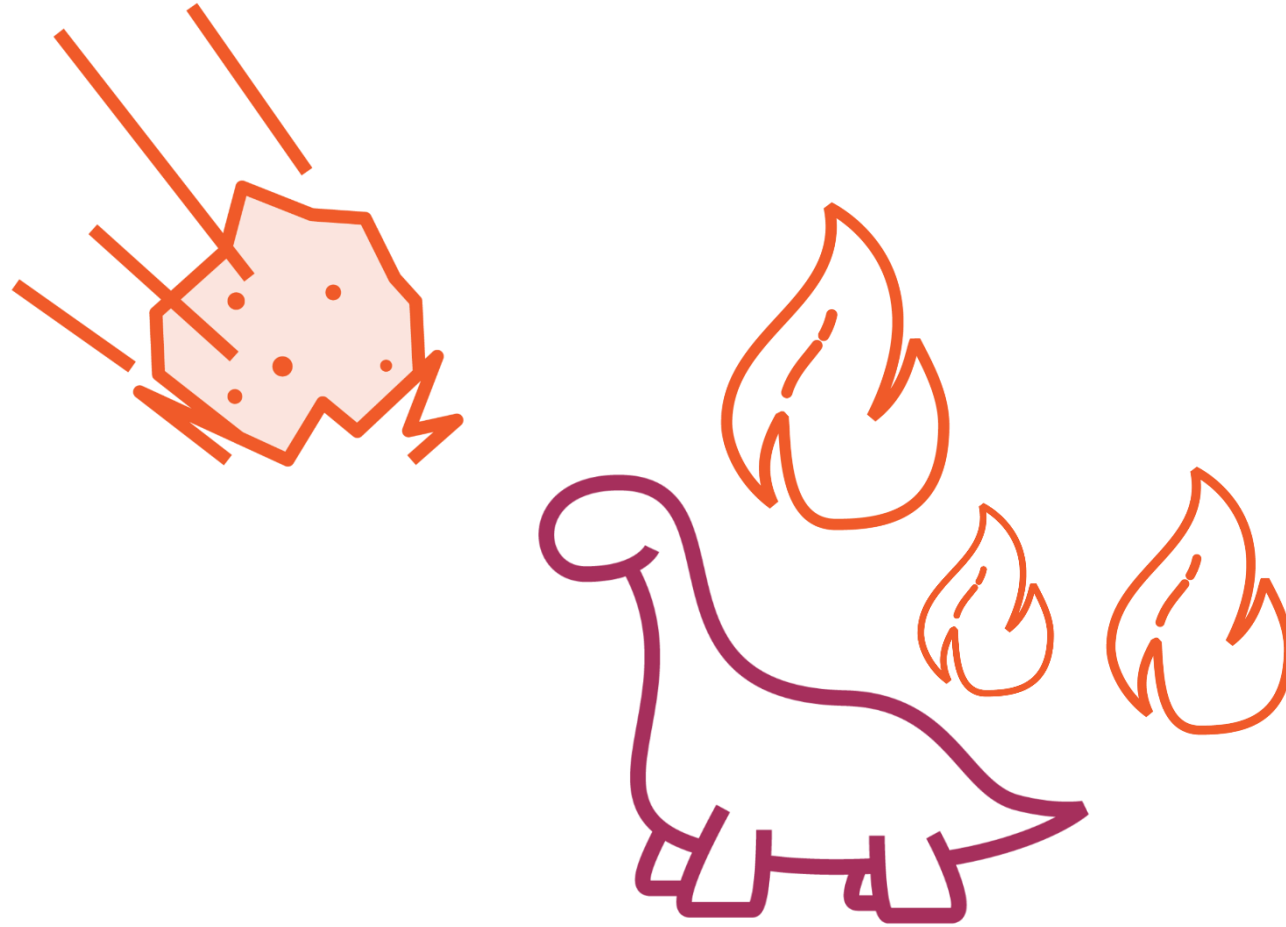
Threat Hunter



The Story Starts and Ends with You

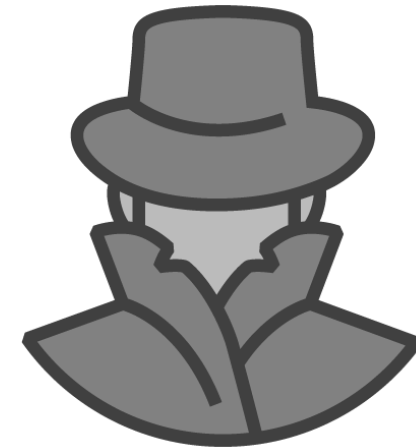
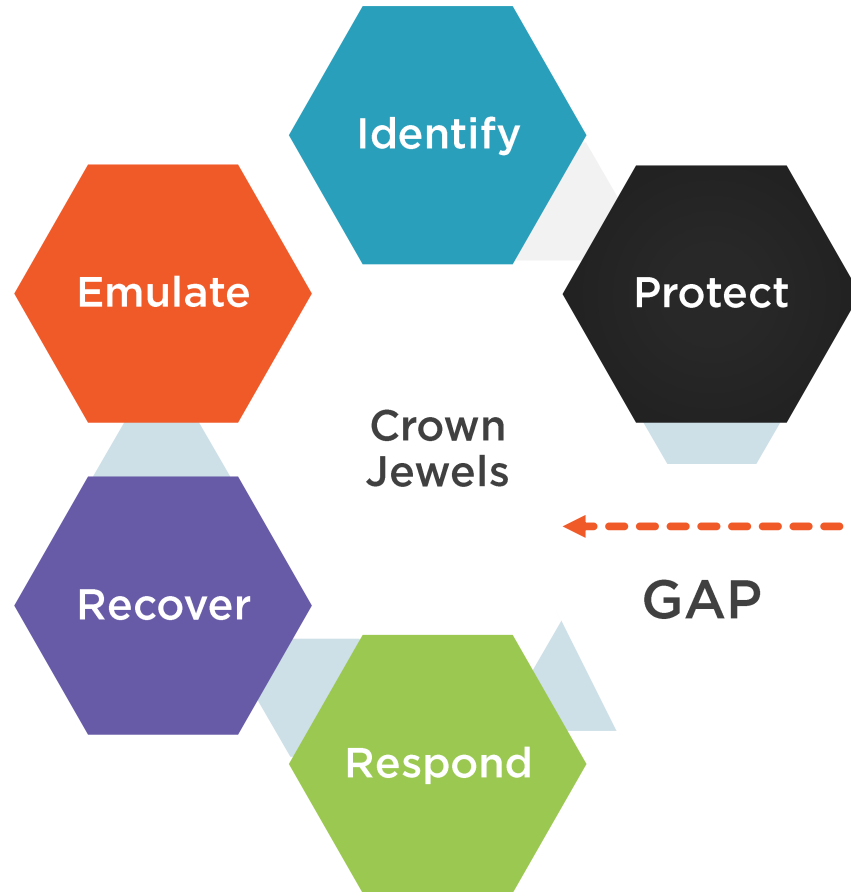


Threat Hunter





Welcome to the Cyber Arms Race





Fighting Technology with Technology

- Dynamic threat landscape
- New tools enhance defense
- Open Source provides efficient initial solution

Fighting Technology with Skills

- Invest in people who stay up to date

Business use case

- NIST CSF functions
- Mitre Att&ck
- Mitre Shield





Thank You



Arkime

OSS Creators



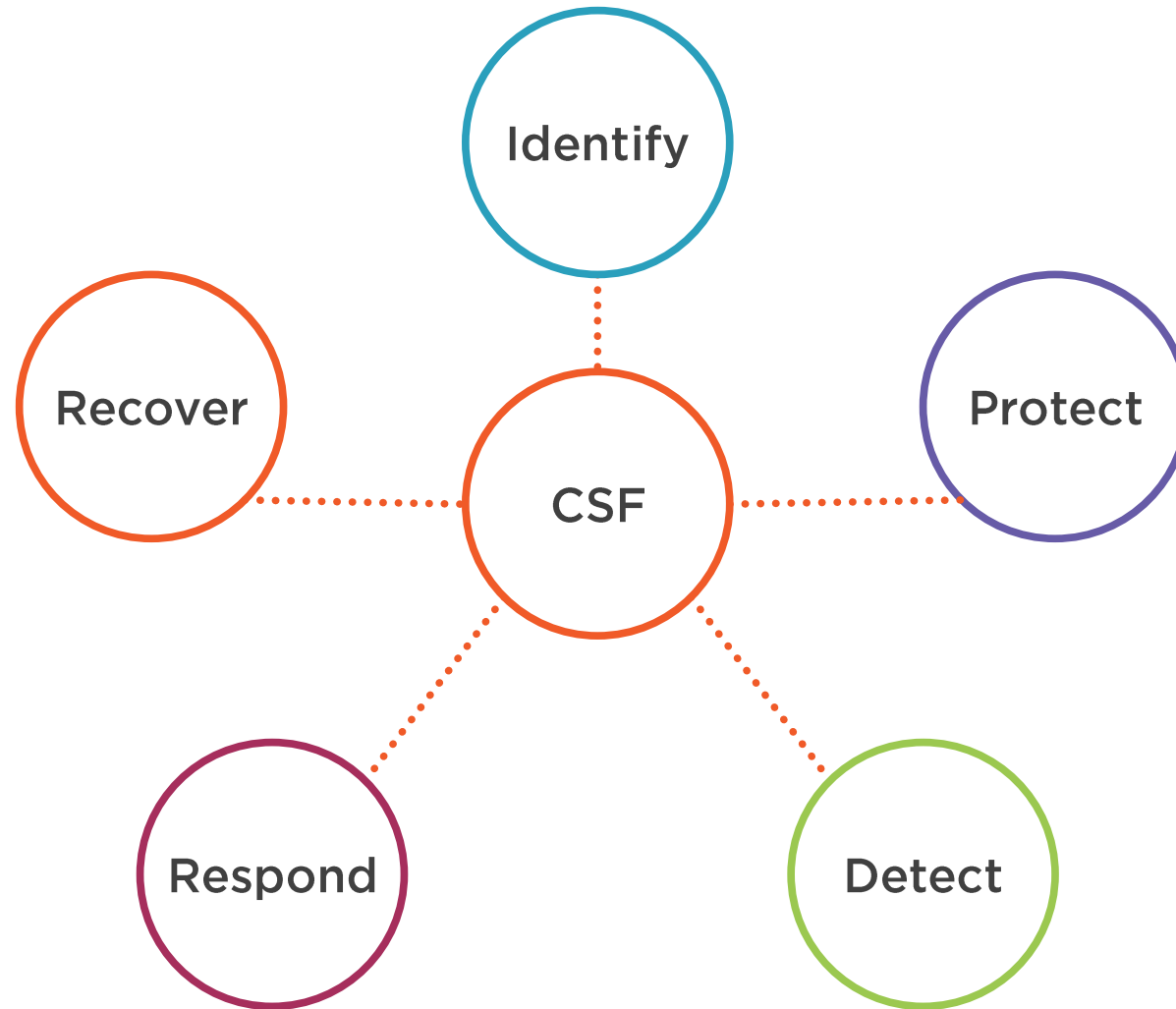
TheHive



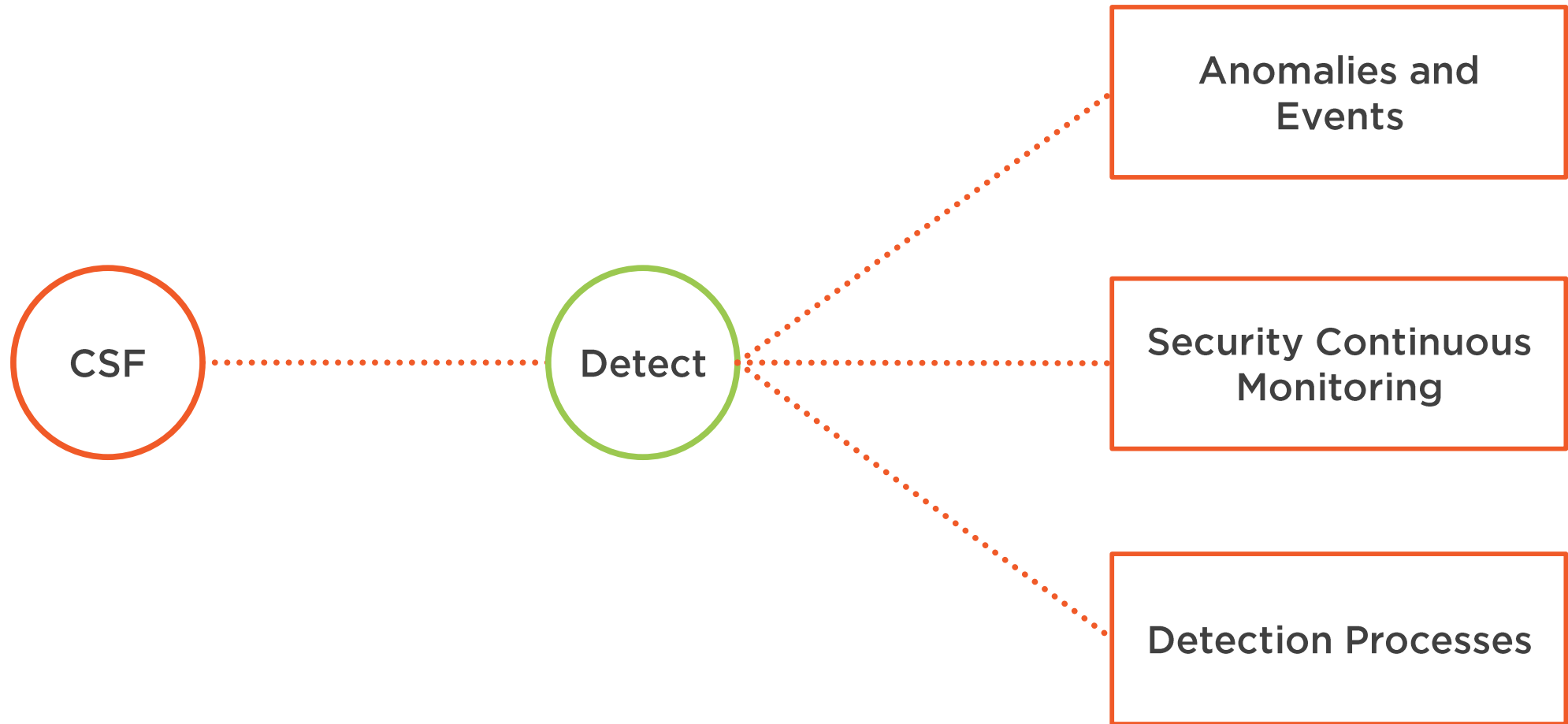
MISP
Threat Sharing



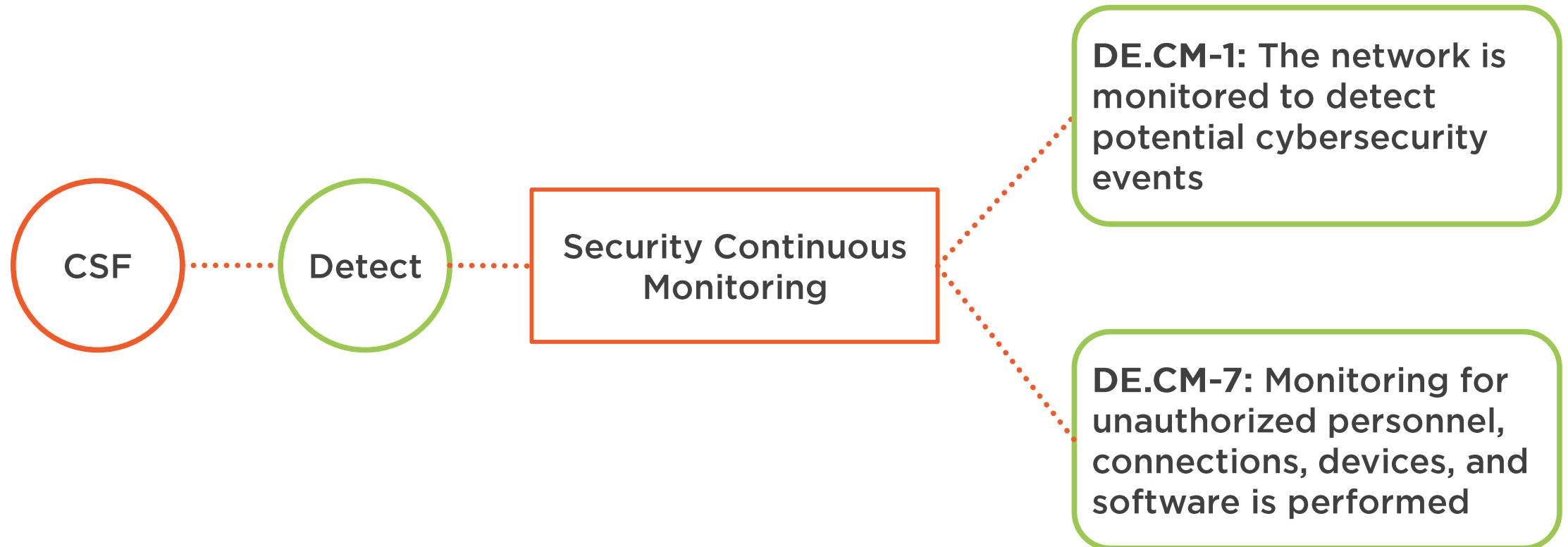
NIST Cybersecurity Framework



NIST Cybersecurity Framework

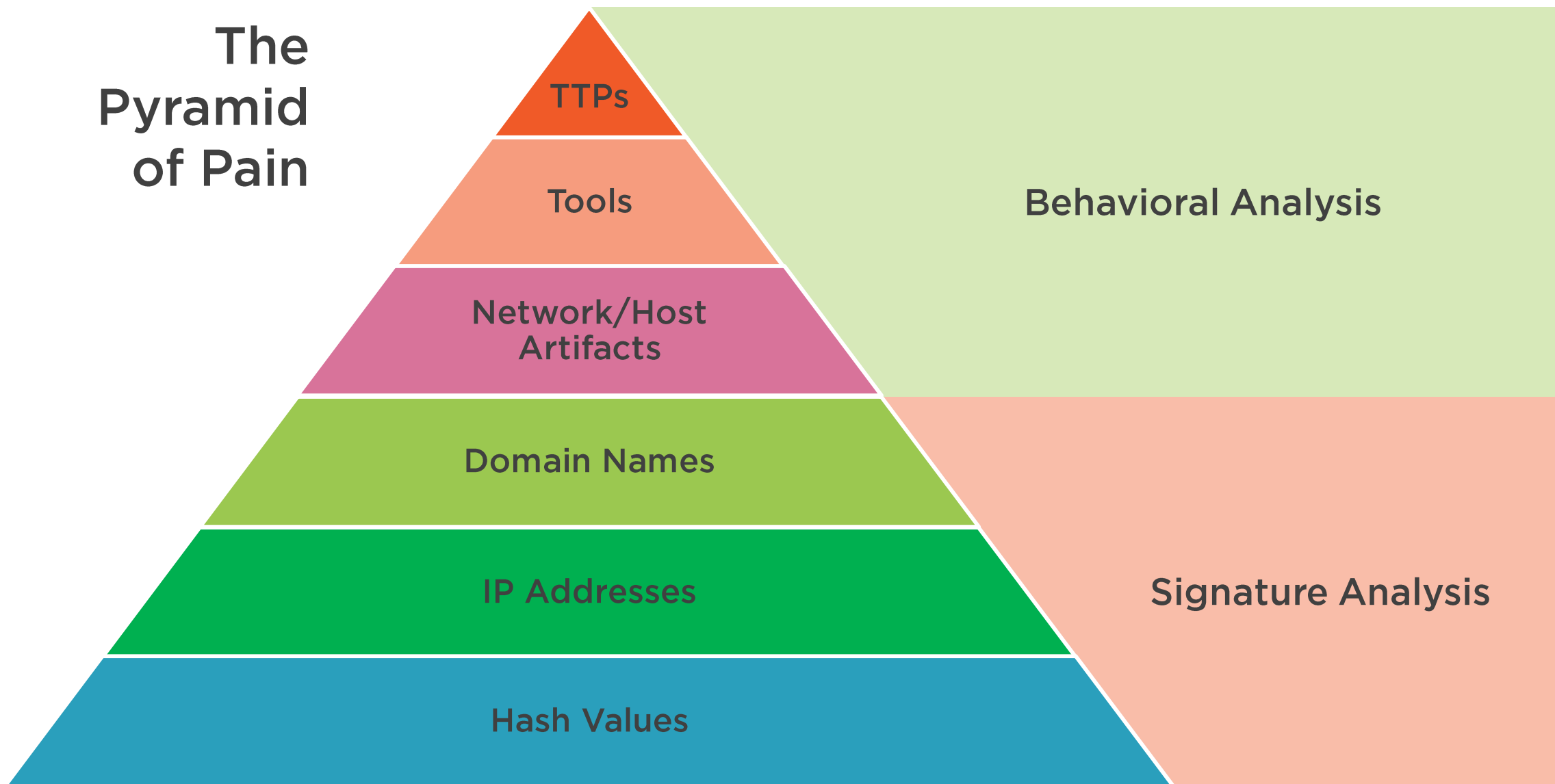


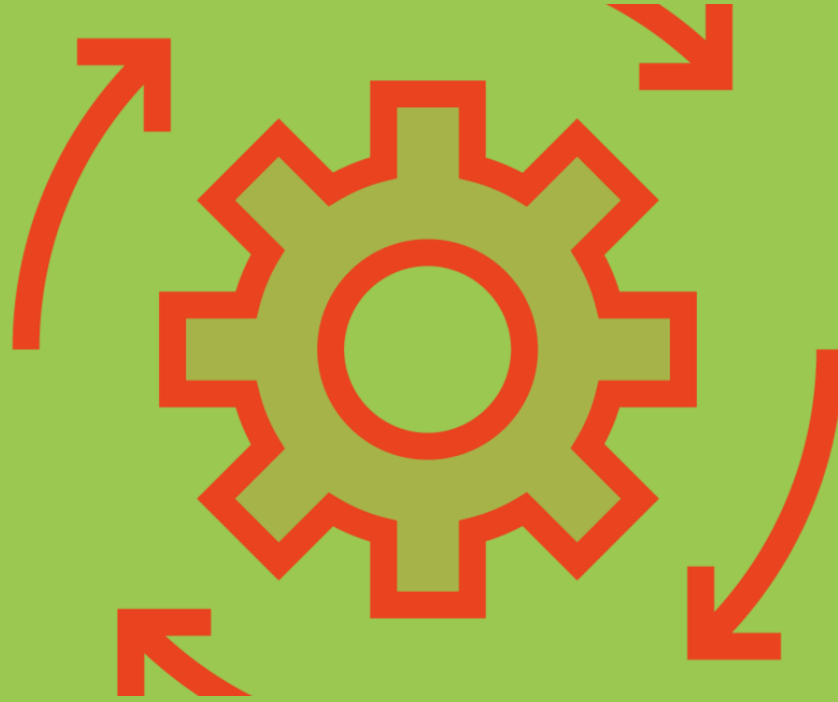
NIST Cybersecurity Framework





The Pyramid of Pain



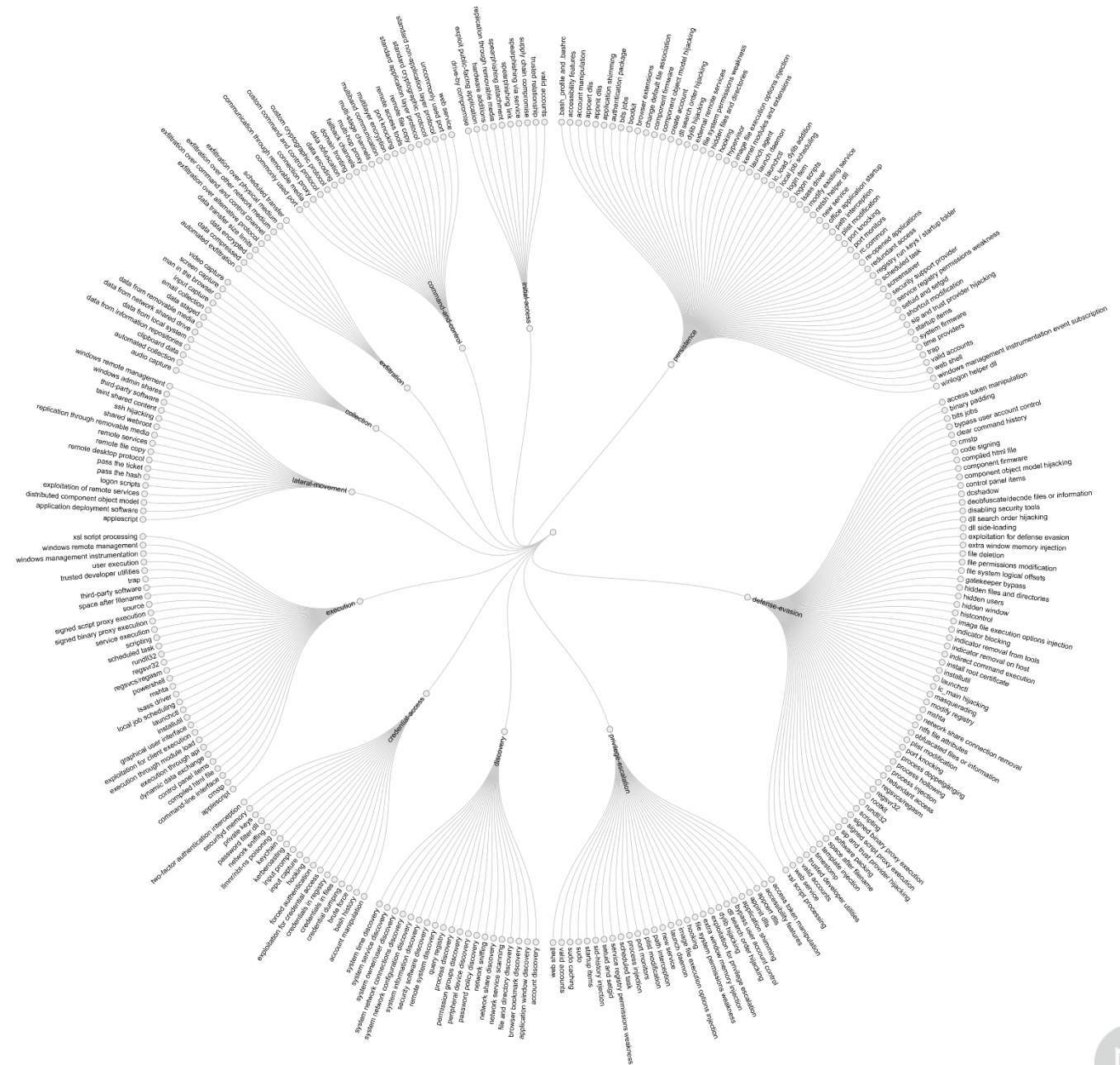


Cyber Security Framework

Enables the communication with management
on how blue team tools mitigate strategic risks
and fulfill audit requirements.



Enter Mitre Att&ck For Defense By Datasource



MITRE ATT&CK

Data Analysis Type

Network Analysis

OS Analysis

Application Analysis

Infrastructure Analysis

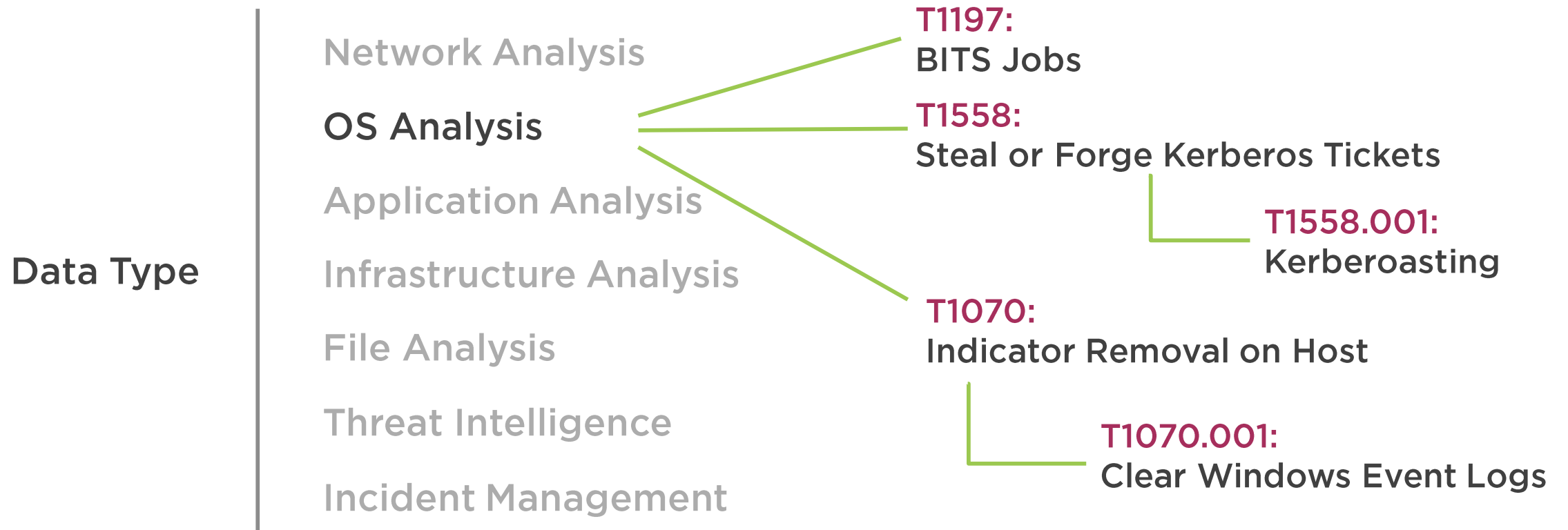
File Analysis

Threat Intelligence

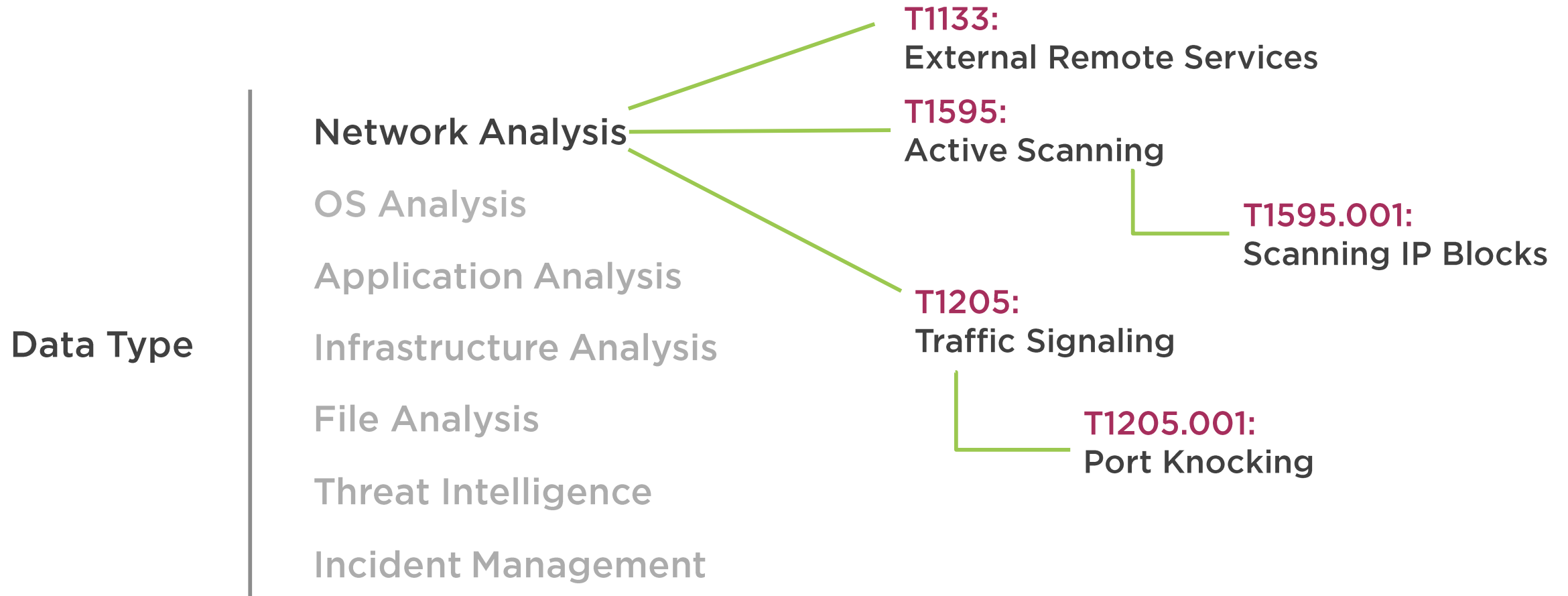
Incident Management



MITRE ATT&CK



MITRE ATT&CK



MITRE ATT&CK

Data Analysis Type

Network Analysis

OS Analysis

Application Analysis

Infrastructure Analysis

File Analysis

Threat Intelligence

Incident Management



MITRE SHIELD

T1133:

BITS Jobs

DTE0032 – Security Controls: A defender can secure Kerberos in order to prevent an adversary from leveraging the tickets to authenticate or move laterally. This may result in the adversary exposing additional TTPs. (DUC0088)

T1595.001:

Steal or Forge Kerberos Tickets

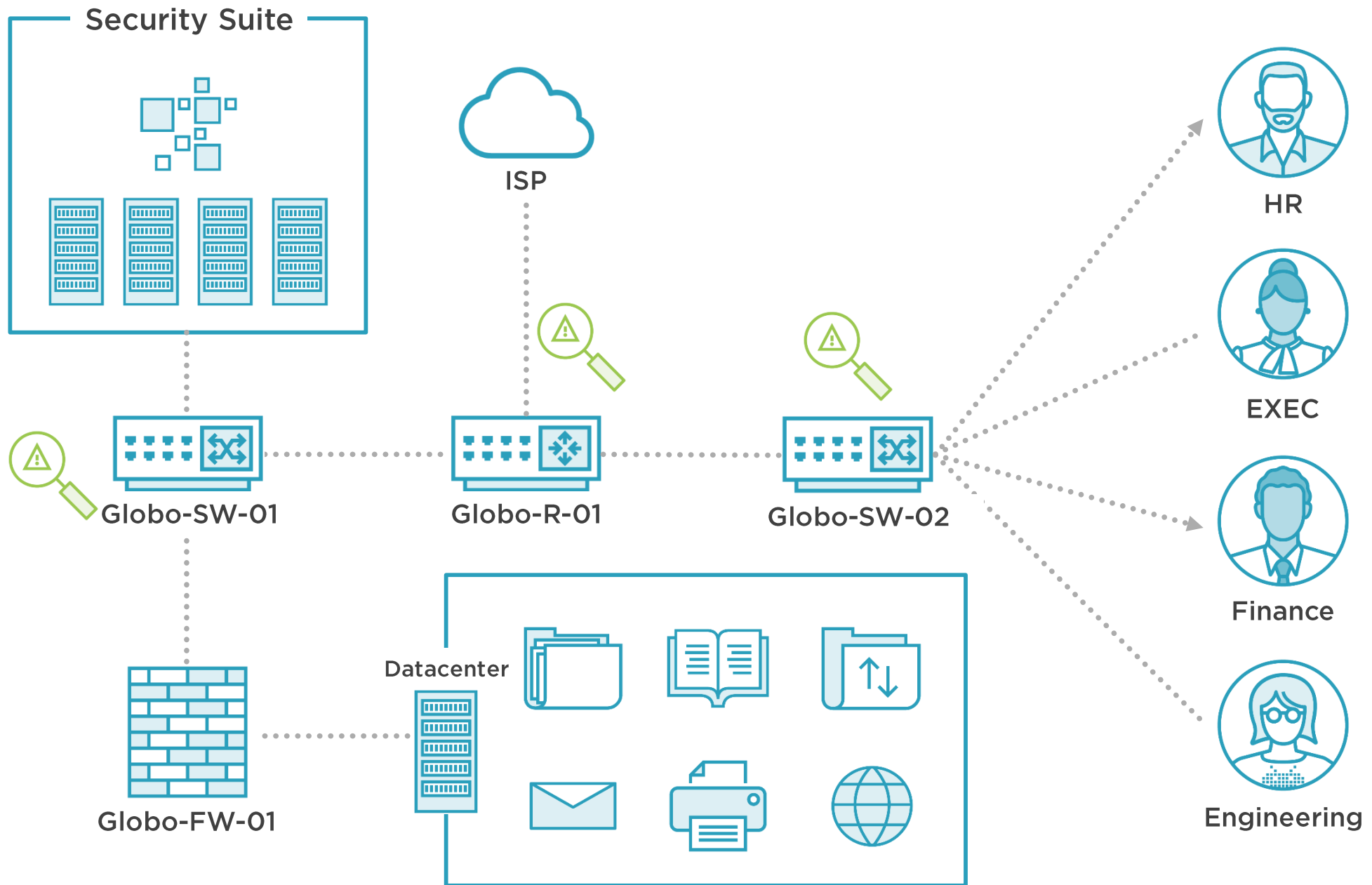
DTE0034 – System Activity Monitoring: By collecting system logs, a defender can implement detections that identify abnormal BITS usage. (DUC0141)

T1070.001:

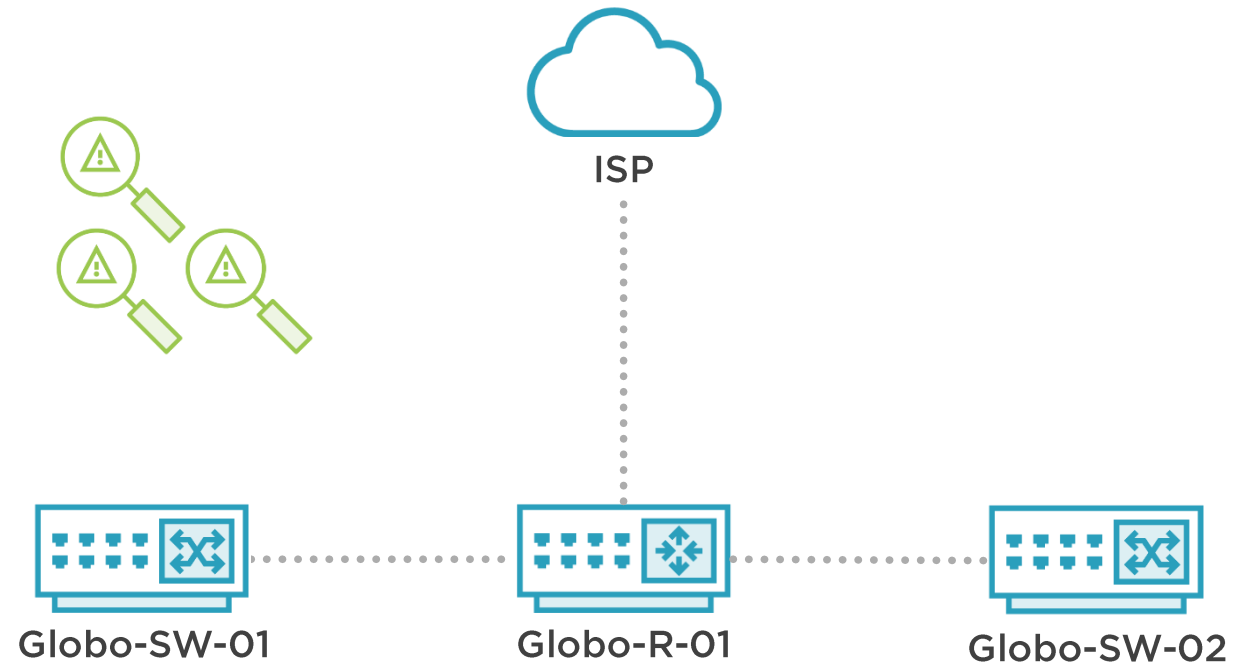
Indicator Removal on Host

DTE0007 – Behavioral Analysis: A defender can look for anomalies in how commands are being executed on a system. This can expose potentially malicious activity. (DUC0221)

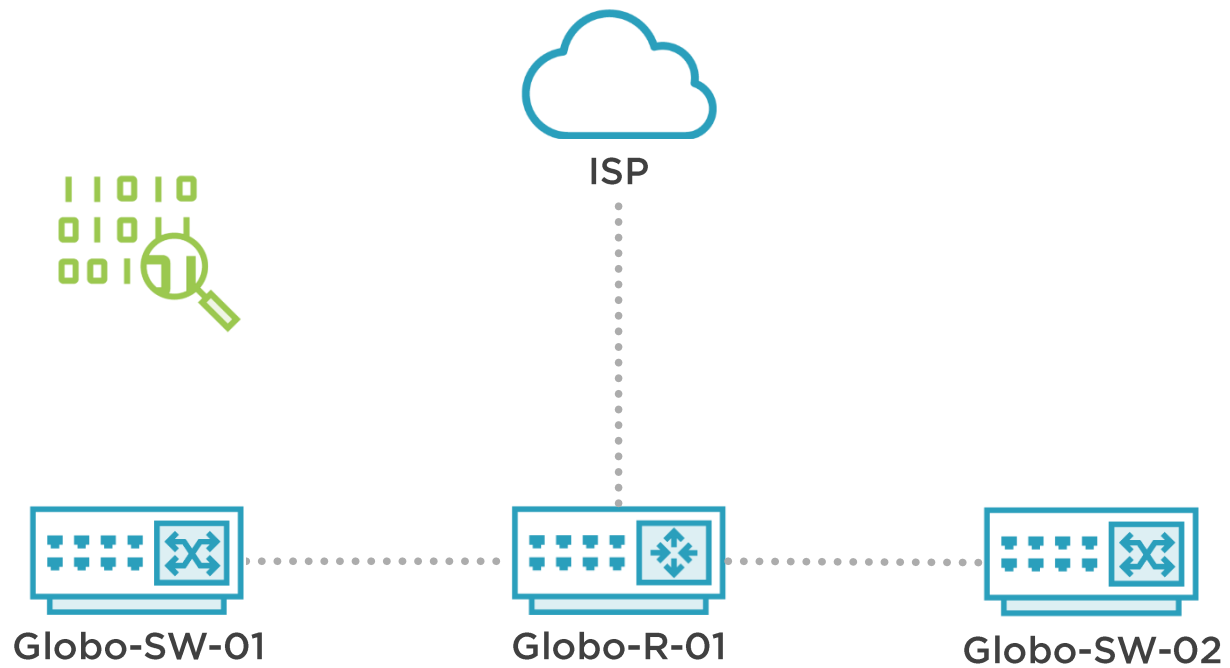


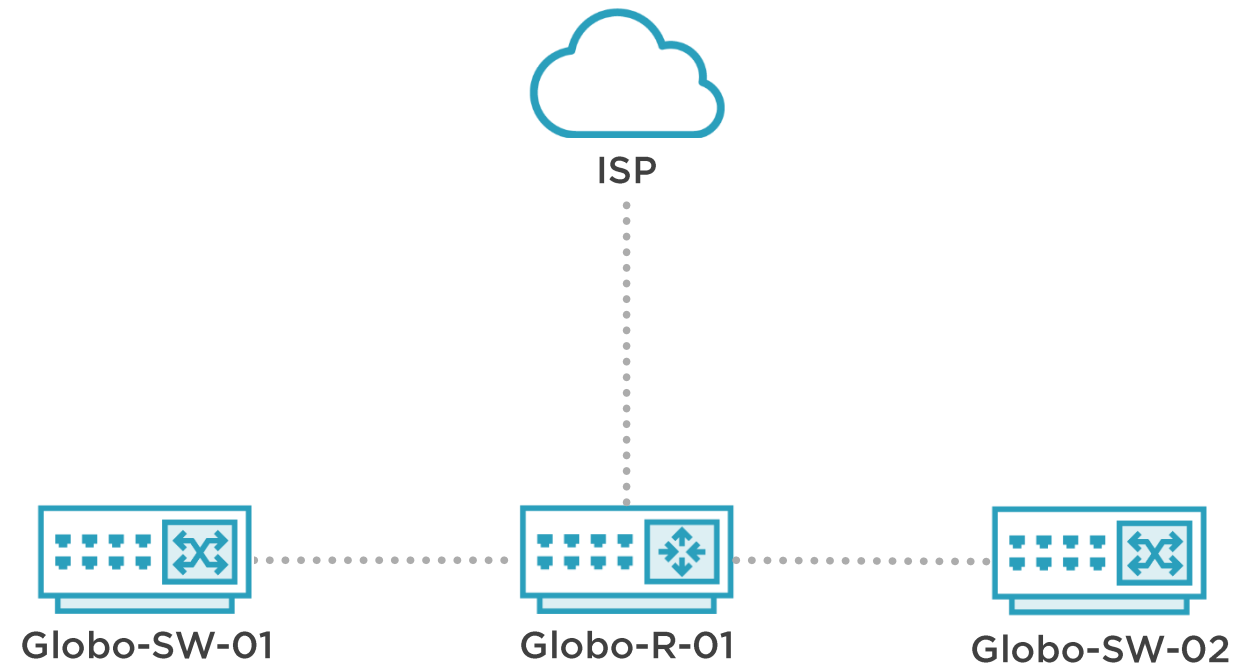
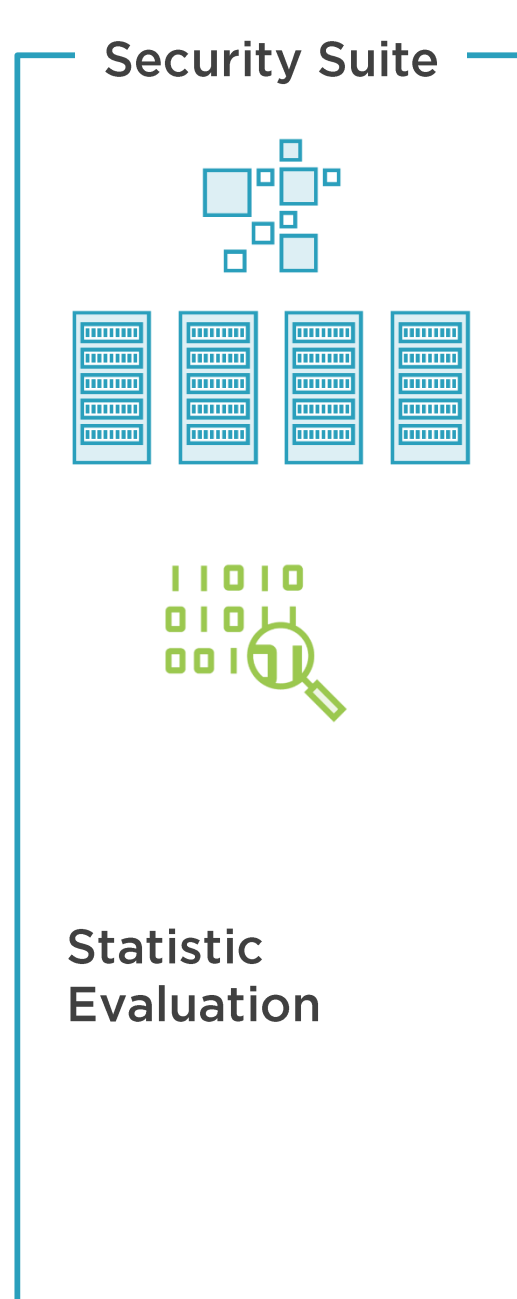


Security Suite



Security Suite





Security Suite



Statistic
Evaluation



ISP



Globo-SW-01

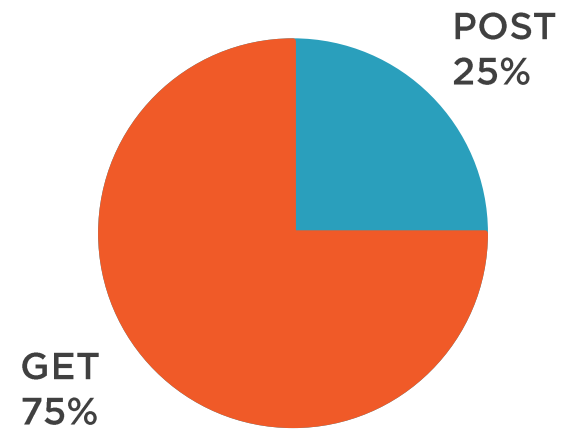


Globo-R-01

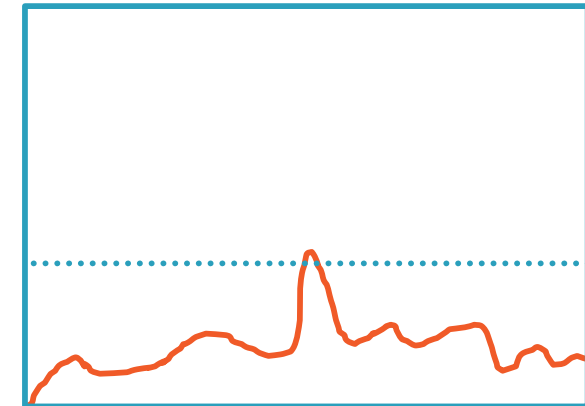


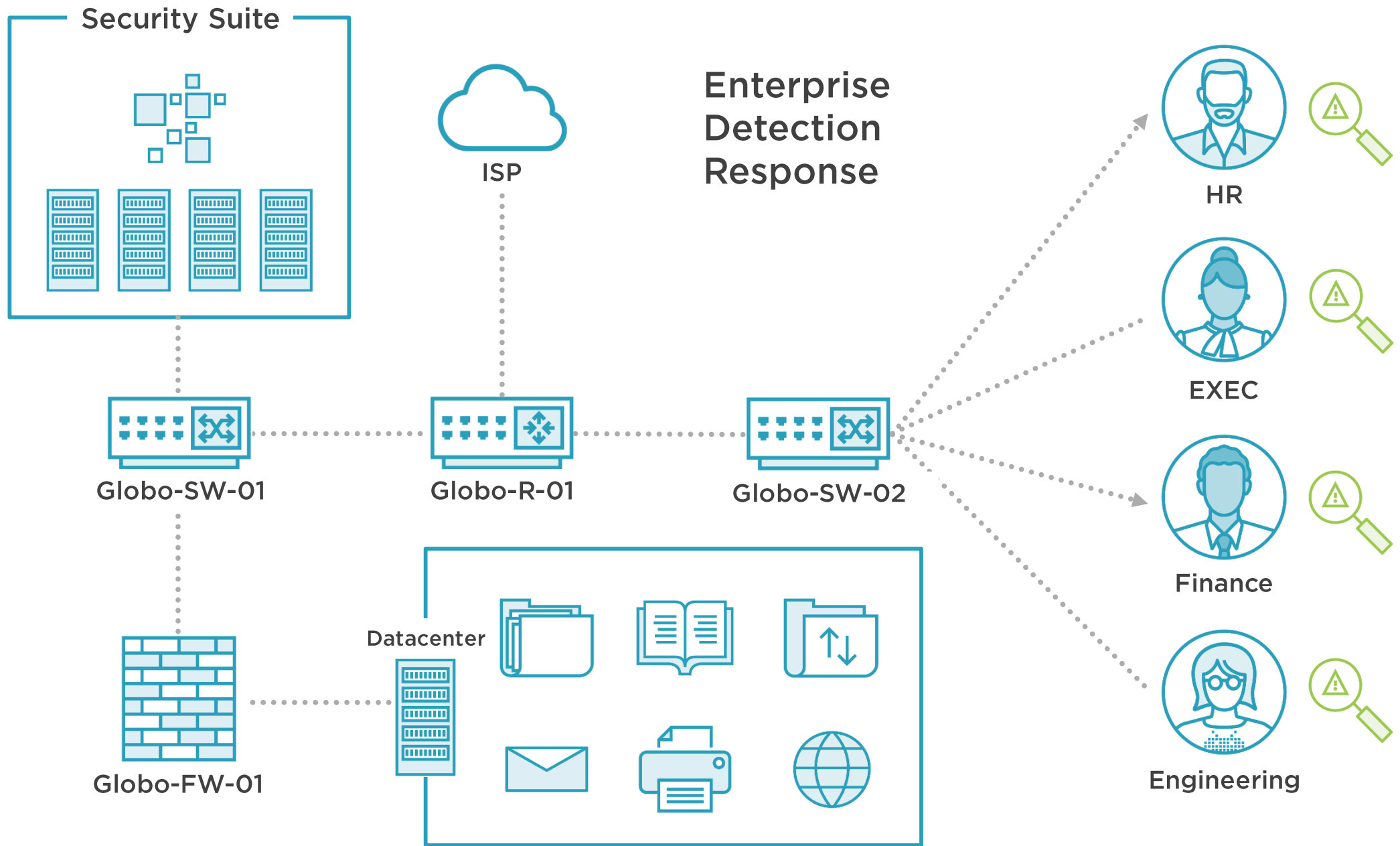
Globo-SW-02

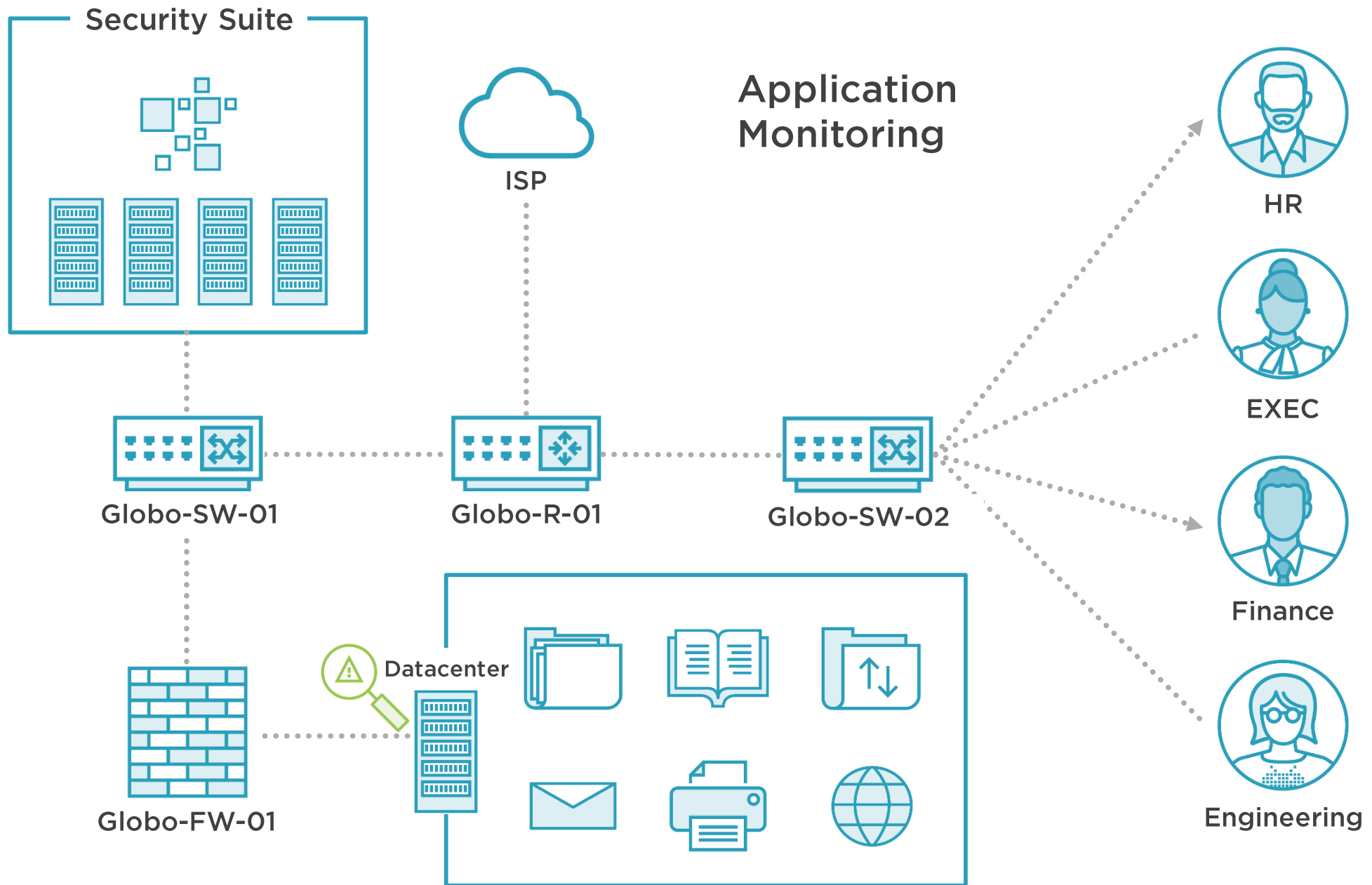
HTTP Methods

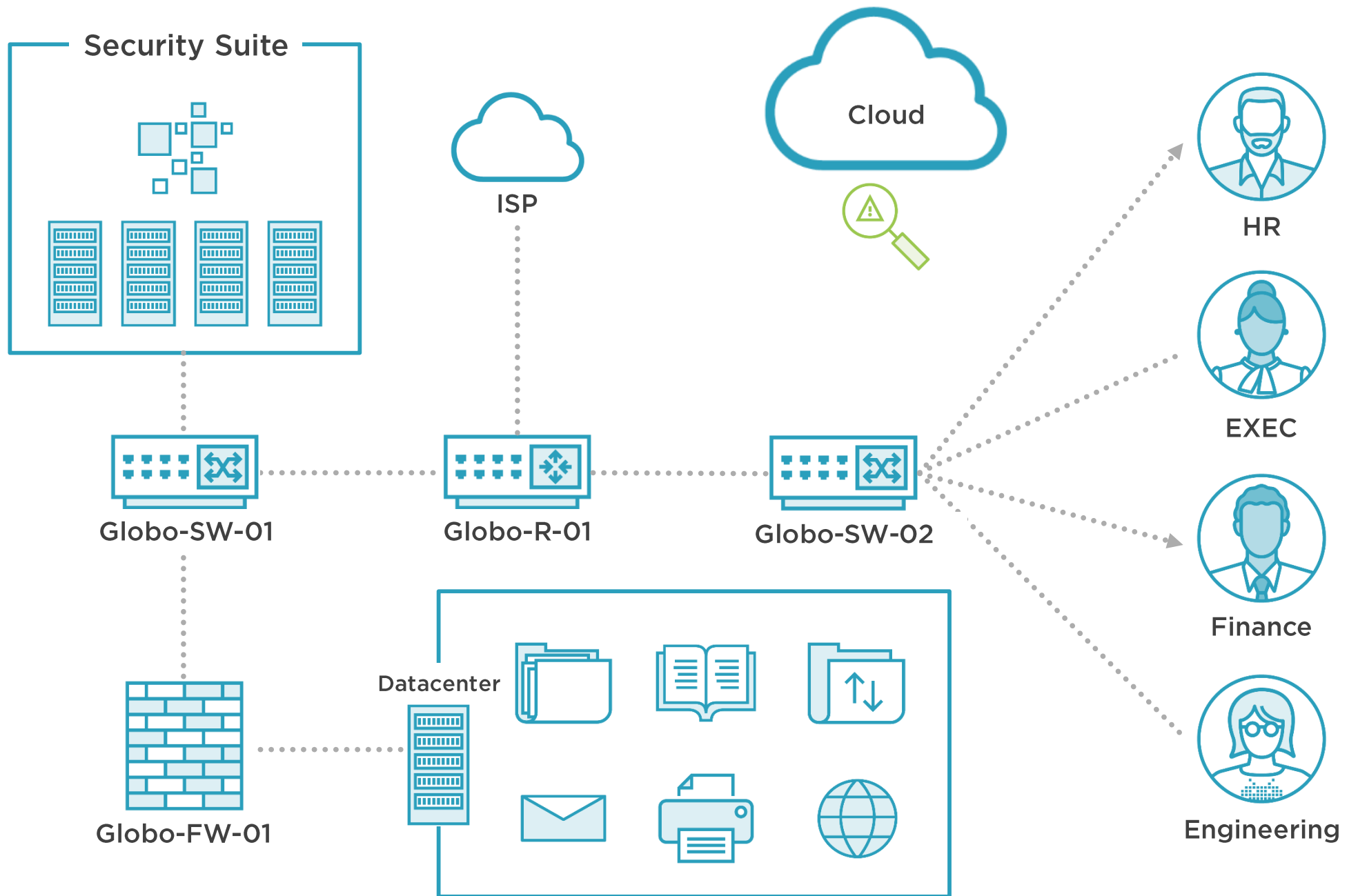


TCP Connection Length









Cybersecurity is a job that must be done right. You are protecting more than just data.



More Information

Capabilities

Scaling Blue Team Tools to the Enterprise

[Getting Started with Zeek | Pluralsight](#)

[Network Security Monitoring \(NSM\) with Security Onion | Pluralsight](#)

[Getting Started with osquery | Pluralsight](#)

Related Information

[MITRE ATT&CK®](#)

[Visualizing ATT&CK. To coincide with RSA this year, we're... | by Andy Applebaum | MITRE ATT&CK® | Medium](#)

[Shield Home \(mitre.org\)](#)

[Red Team Tools for Emulated Adversary Techniques with MITRE ATT&CK | Pluralsight](#)

[Security Event Triage Path | Pluralsight](#)

